Research Article ISSN 2639-8478

Cancer Science & Research

Encryption Gradient of Patients' EMR using Forms of DICOM

Chukwuebuka Regis Anyanwu[1] and Seung Chan Kim[1,2]*

[1]*European University Faculty of Medicine, Tbilisi, Georgia.*

[2]*Yonsei University College of Medicine, Seoul, Republic of Korea.*

***Correspondence:**
Seung Chan Kim, Yonsei University College of Medicine, Seoul, Republic of Korea, Room #205, 2nd floor, 5 Irina Enukidze street, Tbilisi, Georgia, Tel: +82-10-7104-2835.

Received: 04 Oct 2023; **Accepted:** 10 Nov 2023; **Published:** 17 Nov 2023

Citation: Chukwuebuka Regis Anyanwu, Seung Chan Kim. Encryption Gradient of Patients' EMR using Forms of DICOM. Cancer Sci Res. 2023; 6(1): 1-3.

ABSTRACT

Data protection is important. it is especially required for competent patient protection. If it is not done well, it can pose various problems. The problems of leakage can make patients vulnerable. This literally means that the healthcare environment can be threatened in this aspect. DICOM is a digitalized image compression technique using radiologic materials. It restores CT, PET-CT, and X-ray images in order to gain a specific image. It is then compiled to be sent as PACS. These imaging techniques use matrix as a data presenting method. However, it is sent in a linear form. It does not mean that it is not protected, but it means that there are various risks to be managed. In our report, we review that, in the future, a double layer of encryption with patient voice can dramatically evolve the probability of accessing patient healthcare data. This can also be applied in EMR or EHR in the future. The limitations of this study are that there are still risks of cyber-attack. The DDoS can totally make the system function down. However, we see this as a different problem as this is an electronic source matter rather than a hack of preserved data.

Keywords
DICOM, Encryption, Voice Recognition, Matrix.

Introduction

"DICOM" is a password that can be made by controlling digitalized images. It is to present data of radiological diagnosis and to give major findings [1,2]. Nevertheless, the potential leakage of this data can be a major cause for concern in the healthcare environment. In 2020, there was a data leak in DICOM [3]. This existential issue makes patients vulnerable and in turn, depletes the trust and confidence that patients should otherwise foster with their health providers and the systems already in place.

How do medicine and society differ? Many countries have established medical insurance and social insurance policies since the 1970s. However, few countries accepted national social insurance and medical insurance in 1987. Based on this metric, we deduce that the medical institutions in these countries run based on a mutually beneficial corporation between the medical institutions themselves and the society. Salaries for health care professionals are paid for from the money provided by society. This usually falls within the purview of the Health Insurance Review and Assessment Service. In this respect, it is not just a mutually beneficial relationship but an inseparable relationship. This can be likened to the "Quantum Brownian motion". This study corresponds to the first stage of encryption [5-8]. A sure solution can be obtained from DICOM in light of our review. Just as one can theoretically explore the navigational principles of the world with mathematical and statistical techniques, DICOM will provide the best way of living a life that is safe and secure with regards to data security [9-11].

Materials and Methods

DICOM analysis

DICOM is a perfect data storage machine that exists in the background of the data of personal biological information. It serves to transform by way of PACS system. In this system, multiple variables are multiplied in a new transformation array, which would be four times denser. There, a new value is added to the new array, which restores the information when needed. This order is kept in a separate array in the same way that pixel value is multiplied. This way, encryption always makes a protected copy of the data that is impregnable.

Voice Recording and Keeping as a Source of Sound Waves

Voice is a message that is very personal. Voice recognition technology has already been advanced greatly in this era. These advancements can be adapted and implemented to find and match people's data. Consent then becomes very key because if there is no individual consent provided to use of one's voice, it becomes hard to access data from other people. This is one of the highest levels of data security.

Voice Recognition Technique

Improving the quality of encryption is another crucial step towards enhancing patient privacy. If a patient's password can be deciphered even through dark means, it loses its essence as a password. By aligning this notion with our encryption methods, we can incorporate supplementary measures to safeguard data. This prospect can be explored further through clinical trials and applications.

The voice recognition process typically involves the following steps:
1) Audio Input: The system captures audio data through a microphone or any other sound input device.

2) Pre-processing: The captured audio may go through pre-processing steps to remove background noise, normalize volume levels, and enhance the quality of the input.

3) Feature Extraction: The system analyzes the pre-processed audio to extract relevant features, which represent different aspects of the speech, such as frequency, duration, and amplitude.

4) Acoustic Modeling: Machine-learning algorithms, like Hidden Markov Models (HMMs) or deep neural networks, are used to map the extracted features to phonemes or basic units of sound in a specific language.

5) Language Modeling: Another set of machine learning techniques is employed to analyze the sequence of phonemes and predict the most likely words or phrases based on the context of the speech.

6) Decoding: The system combines the acoustic and language models to decode the speech and generate the corresponding text output.

To ensure privacy in voice recognition systems, developers and companies take several measures:
1) On-Device Processing: Many voice recognition systems now perform processing and analysis directly on the device, reducing the need to send the raw audio to remote servers. This approach enhances privacy by minimizing the exposure of personal data to external networks.

2) Anonymization: Voice data is often anonymized, meaning that personal information like the speaker's identity or location is stripped from the audio before storage or processing. Instead, the system may use unique identifiers to distinguish users without revealing their actual identities.

3) Data Encryption: Voice data that needs to be transmitted to remote servers or cloud-based processing centers may be encrypted to protect it from unauthorized access during transit.

4) User Consent and Control: Reputable voice recognition systems seek explicit consent from users to collect and process their voice data. Users may also have control over their data, allowing them to manage and delete their recordings.

5) Data Retention Policies: Companies may implement data retention policies that limit how long voice data is stored. Shorter retention periods reduce the risk of potential data breaches or unauthorized access.

6) Regular Audits and Security Measures: Organizations often conduct regular security audits to identify and address potential vulnerabilities in their voice recognition systems.

It is essential for users to be aware of the privacy policies and practices of the voice recognition systems they use and to exercise caution when sharing sensitive information via voice commands or interactions.

Discussion

The biometric password is a way to pass a high-level encryption step that can only be opened through one's unique signal, voice or vein recognition. The main purpose is to exclude the linear combination that prevents it from being pierced by a straight line, so that it cannot be pierced by anything [1-3]. This way, one cannot access medical information all at once. Accessibility of information accessed in this way can only happen legally by the patient's tacit consent, and it can happen to a competent patient. The disadvantage of a normal site or link is that even if it is blockchainized, it is pierced by linear combination [12].

These points should work well and be applied to increase the probability of preventing these errors [13]. Voice recognition of an electronic device from a patient will be very unique to the patient and the needs will be fulfilled with what we can encrypt. These voice recognition techniques are not new. They are formed when they become the best scenario in places. It is legal part of the patient's data protection in the future. The threat of hacking and AI is a global threat and many celebrities have warned the threat of artificial intelligence [14].

The limitations of this study is that there are still risks of cyber attack. The DDoS attack may totally make the system down.

However, we see this as a different problem as this is an electronic source matter rather than a hack of preserved data. Rather, a ransomware is a threat to the protection of data. It is not going backwards when the hacker has the key.

Medical operating systems are used in many places. Data security is as important as it is used in many places, and it requires protection of not only patient privacy but also extensive patient data. In this regard, quantum cryptography has opened up numerous possibilities. Quantum cryptography is known as a password that no hacker can break [15]. Using such strong encryption has the good advantage of being able to develop it using the working principle and energy of Brownian motion without continuously devising prime number-based encryption or encryption techniques. The same is true for dental medical devices. If the operating system is not well equipped, data security of dental data is not secure, and there are cases of viruses. By using encryption technology, it can be used not only for encryption but also for two-way communication. Even in 32-bit communication, even if many communication satellites are developed in the world expanding into space, it can contribute to remote transmission of medical data. On the point of view of cryptographic data developers, the quantity of cryptography is not important because it is qualitative [16,17].

Encrypting itself how to improve its quality is another important step towards strengthening secrecy. There is a huge difference between knowing and not knowing. Being able to decipher the password even in the dark means that it is no longer a password. Only to find that this is similar to our encryption methods, we can have additional voices to protect data. This can be done in further clinical trials and applications.

References

1. Graham RN, Perriss RW, Scarsbrook AF. DICOM demystified: a review of digital file formats and their use in radiological practice. Clin Radiol. 2005; 60: 1133-1140.
2. ahn CE, Carrino JA, Flynn MJ, et al. DICOM and radiology: past, present, and future. Journal of the American Coll Radiol. 2007; 4: 652-657.
3. Desjardins B, Mirsky Y, Ortiz MP, et al. DICOM images have been hacked! Now what? AJR Am J Roentgenol. 2020; 214: 727-735.
4. Riddle WR, Pickens DR. Extracting data from a DICOM file. Medical physics. 2005; 32: 1537-1541.
5. Crane JC, Olson MP, Nelson SJ. SIVIC: open-source, standards-based software for DICOM MR spectroscopy workflows. Int J Biomed Imaging. 2013; 12-12.
6. Halford JJ, Clunie DA, Brinkmann BH, et al. Standardization of neurophysiology signal data into the DICOM® standard. Clin Neurophysiol. 2021; 132: 993-997.
7. Mantri M, Taran S, Sunder G. DICOM integration libraries for medical image interoperability: a technical review. IEEE Reviews in Biomedical Engineering. 2020; 15: 247-259.
8. Robinson JD. Beyond the DICOM header: additional issues in deidentification. AJR Am J Roentgenol. 2014; 203: W658-W664.
9. Law MY, Liu B, Chan LW. DICOM-RT–based electronic patient record information system for radiation therapy. Radiographics. 2009; 29: 961-972.
10. Le AH, Liu B, Huang HK. Integration of computer-aided diagnosis/detection (CAD) results in a PACS environment using CAD–PACS toolkit and DICOM SR. Int J Comput Assist Radiol Surg. 2009; 4: 317-329.
11. Medina García R, Torres Serrano E, Segrelles Quilis JD, et al. A systematic approach for using DICOM structured reports in clinical processes: focus on breast cancer. J Digit Imaging. 2015; 28: 132-145.
12. Rojas-López JA, Fotinós J, Maddalozzo N. Dicomhandler: Python tool for manipulating DICOM files and its application for radiosurgery. Software Impacts. 2023; 16: 100487.
13. Caffery LJ, Rotemberg V, Weber J, et al. The role of DICOM in artificial intelligence for skin disease. Front Med. 2021; 7: 619787.
14. Dorgham O, Naser MA, Ryalat MH, et al. U-NetCTS: U-Net deep neural network for fully automatic segmentation of 3D CT DICOM volume. Smart Health. 2022; 26: 100304.
15. Hardiyanti Y, Pratama SH, Barasabha T, et al. A Study of Water Phantom Homogeneity from DICOM CT-Images Based on Image. J Nucl Tech Appl Sci. 2020: 8: 179-186.
16. KNOLL Florian, Jure Z, Anuroop S, et al. fastMRI: A publicly available raw k-space and DICOM dataset of knee images for accelerated MR image reconstruction using machine learning. Radiol Artif Intell. 2020; 2: e190007.
17. Saraiva AA, de Oliveira MS, de Moura Oliveira PB, et al. Genetic algorithm applied to remove noise in DICOM images. Journal of Information and Optimization Sciences. 2019; 40: 1543-1558.

© 2023 Regis Anyanwu C, et al. This article is distributed under the terms of the Creative Commons Attribution 4.0 International License